IN THE CLAIMS:

Please amend the claims to correspond with the following list. The canceled claims are canceled without prejudice or disclaimer of any subject matter.

1-22. (Canceled)

23. (Currently Amended) A method for verifiably transmitting an electronic package from a sender to a recipient through a certifying authority via a public communications network, the method comprising the steps of:

logging the sender on to a certifying authority using a standard authentication protocol;

creating by the certifying authority an electronic package from inputs transmitted by the sender via the public communications network;

storing by the certifying authority the inputs relating to the electronic package on a server operated by the certifying authority for use in later verifying the inputs relating to the electronic package and storing any other data received from the sender;

delivering a message relative to the electronic package from the certifying authority to the recipient via the public communications network;

~~lagging~~ logging the recipient on to the certifying authority as a response to the receipt of the message;

after logging the recipient on to the certifying authority, generating by the certifying authority an encrypted hash value based on the inputs relating to the electronic package and the delivery thereof, the encrypted hash value uniquely identifying the particulars relating to the electronic package and the delivery thereof; and

transmitting an electronic certificate of service from the certifying authority via the public communications network, the electronic certificate of service including selected inputs relating to the electronic package and ~~a digital certificate~~ the encrypted hash value generated by the certifying authority after logging the recipient on to the certifying authority.

2

24. (Previously Presented) The method of claim 23 further comprising the steps of: storing the electronic package inputs and other related data on the server operated by the certifying authority for use in later producing a duplicate of the electronic package for a period of time agreed upon by the certifying authority and the sender; and

storing the inputs comprising: the name and address of the email sender, the name and address of the recipient, the name and email of the address of any other persons to whom the certificate of service has been delivered, the time of delivery, the date of delivery, the subject of the message, the size of the message, the electronic package retention expiration date, the name of each attachment, and the size of each attachment.

25. (Previously Presented) The method of claim 23 wherein the certifying authority embeds the digital certificate on the face of the electronic certificate of service.

26. (Previously Presented) The method of claim 23 wherein the certifying authority embeds the digital certificate in the electronic certificate of service electronically.

27. (Previously Presented) The method of claim 23 wherein a recipient, sender or other person requests the certifying authority to employ the digital certificate embedded within the electronic certificate of service so as to verify that the contents of the electronic package stored on the certifying authority's server are identical to the description thereof found on the face of the electronic certificate of service.

28. (Previously Presented) The method of claim 23 wherein the certifying authority utilizes the embedded digital certificate within the electronic

certificate of service to locate and identify the electronic package.

29. (Previously Presented) The method of claim 23 wherein the certifying authority, having located and identified the electronic package, reproduces the electronic package identically to that first assembled by the certifying authority.

30. (Previously Presented) The method of claim 23 wherein the reproduced electronic package is certified to be a true and correct copy of the original electronic package, such certification being made by the certifying authority.

31. (Previously Presented) The method of claim 23 wherein the certifying authority issues a certification to a requesting party that the reproduced electronic package is a true and correct copy of the original electronic package and said certification and electronic package are delivered to said requesting party.

32. (Currently Amended) The method of claim 23 wherein ~~the particulars surrounding the electronic package comprises maximum number of days within which to deliver the electronic package to the recipient~~ the electronic certificate of service is transmitted to a recipient from the certifying authority via the public communications network within a predetermined number of days after the certifying authority assembles an electronic package from inputs transmitted by the sender via the public communications network.

33. (Previously Presented) The method of claim 32 further comprising the step of informing the sender, in event that delivery was not made to the recipient within the maximum number of days, by delivering to the sender and other appropriate persons, an electronic certificate of non-service.

34. (Previously Presented) The method of claim 23 wherein the particulars surrounding the electronic package comprises a date through which the electronic package is to be stored by the certifying authority.

35. (Previously Presented) The method of claim 23 wherein tracked message includes an email message and an email attachment and wherein the particulars surrounding the electronic package comprises identity of sender, email address of sender, identity of recipient, email address of recipient, date of transmission, time of transmission, length of the email message, name of the email attachment, and size of the email attachment.

36. (Previously Presented) The method of claim 23 further comprising the steps of creating the electronic certificate of service as an encrypted file.

37. (Previously Presented) The method of claim 23 wherein the step of creating the electronic certificate of service as an encrypted file is accomplished by creating an encrypted PDF file that is printable but not modifiable.

38. (Previously Presented) The method of claim 23 further comprising the step of verifying an encrypted hash value that is questioned by transmitting the encrypted hash value to the certifying authority; and comparing the encrypted hash value that is questioned with records of the certifying authority.

39. (Previously Presented) The method of claim 23 further comprising the step of notifying the recipient via the public communications network that the electronic package is available for pickup from the server operated by the certifying authority.

40. (Previously Presented) The method of claim 38 wherein the step of

5

delivering the electronic package from the certifying authority to the recipient via the public communications network occurs upon a request for download thereof by the recipient; and wherein the step of transmitting an electronic certificate of service from the certifying authority via the public communications network takes place after completion of the delivering step.

41. (Previously Presented) The method of claim 23 wherein particulars of the inputs of the recipient that are converted to an electronic package by the certifying authority are encrypted using an encrypted key maintained solely by the certifying authority for the purpose of embedding the same into the electronic certificate of service.

42. (Previously Presented) The method of claim 23 wherein the step of transmitting an electronic certificate of service transmits an electronic certificate of service to the sender.

43. (Previously Presented) The method of claim 23 wherein the step of transmitting an electronic certificate of service transmits an electronic certificate of service to the recipient.

44. (Previously Presented) The method of claim 23 wherein the step of transmitting an electronic certificate of service transmits an electronic certificate of service to a designee of the sender other than the recipient.

45. (New) A method for verifiably transmitting an electronic package from a sender to a recipient through a certifying authority via a public communications network, the method comprising the steps of:

at a certifying authority, verifying a sender's account status with the certifying authority;

posting information to a transaction log up of the certifying authority, the information including the name of a sender, the name of a recipient, and the identity of an electronic package received by the certifying authority from the sender;

storing an electronic package received at the certifying authority from the sender;

sending information to the sender indicating that the electronic package has been received by the certifying authority;

sending an electronic correspondence to the recipient that an electronic package is addressed to the recipient and is available at the certifying authority;

receiving a request at the certifying authority from the recipient for retrieving the electronic package;

verifying the identity of the recipient at the certifying authority;

delivering the electronic package to the recipient;

after receiving a request at the certifying authority from the recipient, generating an encrypted hash value based on particulars relating to the delivery of the electronic package to the recipient and the content of the electronic package; and

generating an electronic certificate of service with identifiers related to the delivery of the electronic package to the recipient and the content of the electronic package.

46. (New) The method of claim 45 wherein generating an encrypted hash value is also based on an in camera key.

47. (New) The method of claim 45 further comprising:

Sending a URL in an email to the recipient, the URL for logging onto the certifying authority.

48. (New) The method of claim 45 further comprising:

entering a message code at the certifying authority to confirm the authenticity of recipient.

49. (New) The method of claim 45 further comprising:

sending the electronic package to the recipient with a JAVA applet.

50. (New) The method of claim 45 further comprising:

sending the electronic package to the recipient in an email after receiving a request from the recipient.

51. (New) The method of claim 45 wherein the delivery of :

the electronic package to the recipient is as a download.

52. (New) The method of claim 45 wherein the electronic package received by the certifying authority from the sender includes an acsii file.

53. (New) The method of claim 45 wherein the electronic package received by the certifying authority from the sender includes a binary file.

54. (New) The method of claim 45 wherein the electronic package received by the certifying authority from the sender includes an email attachment.